An Oracle White Paper
January, 2015

Enterprise Manager Cloud Control 12*c*: Configuring External User Authentication Using Microsoft Active Directory

Table of Contents

Executive Overview

Oracle Enterprise Manager is Oracle's integrated enterprise IT management product line and provides the industry's first complete cloud lifecycle management solution. Oracle Enterprise Manager's Business-Driven IT Management capabilities allow you to quickly set up, manage and support enterprise clouds and traditional Oracle IT environments from applications to disk. Enterprise Manager allows customers to achieve:

- *Best service levels for traditional and cloud applications* through management from a business perspective including Oracle Fusion Applications
- *Maximum return on IT management* investment through the best solutions for intelligent management of the Oracle stack and engineered systems
- *Unmatched customer support experience* through real-time integration of Oracle's knowledgebase with each customer environment

Introduction

The dynamic and complex nature of today's IT environments, coupled with stringent regulatory requirements make security a critical area of consideration for both business and IT managers in their managed environments. Key security considerations encompass applications and the entire IT infrastructure in many areas including, but not limited to, data protection, communication and application protection. Another common security area of consideration is user authentication.

User authentication is a focus area for many security professionals. User authentication is the process of determining the validity of a user accessing an application or system. IT security teams generally invest considerably in an authentication scheme as an organizational standard and assess tools and applications, based on their user authentication compatibility with that company standard.

The default method of user authentication for Enterprise Manager is repository based user authentication. Enterprise Manager also offers the flexibility of integrating with many popular identity management systems in a process defined as external authentication.

This white paper outlines the integration of Enterprise Manager with one of the most common identity management authentication schemes among our customers - Microsoft Active Directory. We will discuss our one-step configuration command and then iterate through the steps to validate that the set up is correct and complete.

Note: *This white paper assumes that you are familiar with the Administration of Microsoft Active Directory, Oracle WebLogic Server and Oracle Enterprise Manager. For detailed information, see the Microsoft Active Directory Documentation on MSDN, the Oracle Enterprise Manager Cloud Control Administrator's Guide and Enterprise Manager Security Guide*.

External Authentication

User authentication is the process of determining the validity of a user. Enterprise Manger user authentication is the process of determining the validity of a user accessing Enterprise Manager, either via the Console or Enterprise Manager Command Line Interface, EM CLI.

The default method of user authentication for Enterprise Manager is repository based user authentication. Repository based user authentication is provided out of the box and compares a user password to one stored in the Oracle Management Repository database. The Oracle Management Repository, OMR is used as a persistent data store. Examples of the information stored in the repository include job definitions, user information, monitoring and alerting settings and all configuration and monitoring data related to managed targets. The Oracle Management Service coordinates and communicates with all the components of Enterprise Manager. The Oracle Management Service cannot run if the repository is unavailable. The Oracle Management Repository is the source of truth for Enterprise Manager.

Enterprise Manager also offers the flexibility of integrating with many popular identity management schemes in a process defined as external authentication. During external authentication Enterprise Manager delegates user authentication to the WebLogic Server. During external authentications WebLogic Server communicates with an external source such as Oracle Access Manager, LDAP, and Active Directory etc. to perform the user authentication. WebLogic Server is installed with Enterprise Manager.

For the extensive list of authentication providers supported by WebLogic Server please see the Oracle Fusion Middleware Online Documentation for WebLogic Server.

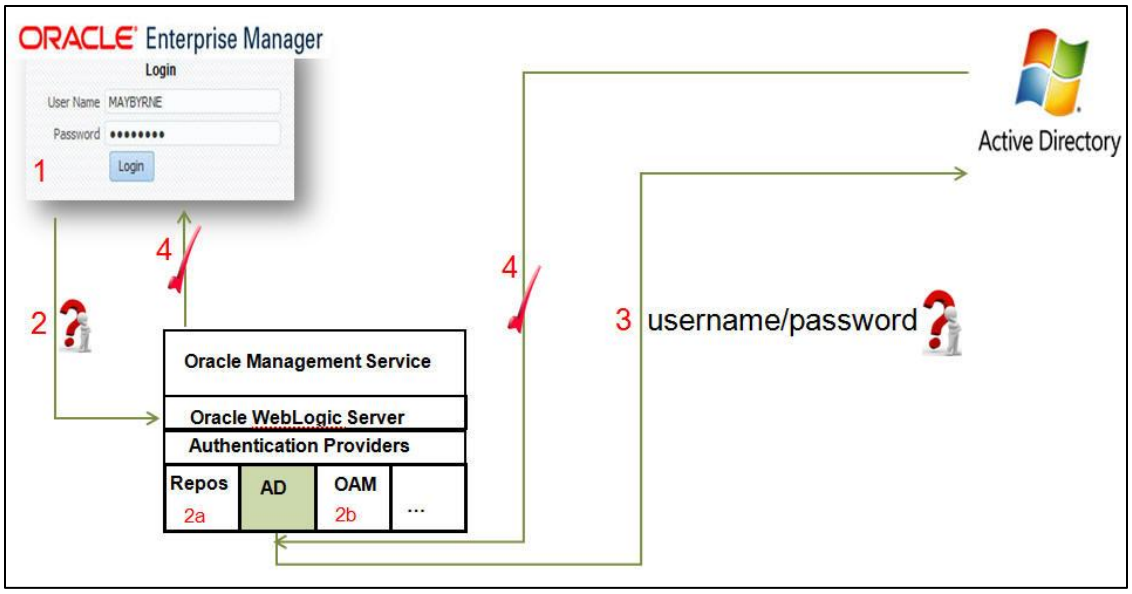

Figure 1: Enterprise Manager User Authentication using Active Directory

The diagram gives a high level pictorial representation of the flow during external user authentication.

1. The user is prompted to enter their username and password.
2. The username and password are sent to the WebLogic Server via the Oracle Management Service, OMS. The WebLogic Server sends the user name and password to the appropriate authentication identity store, based on a pre configured authentication provider. Active Directory in our example.

   In this diagram the WebLogic Server is also configured with

   2a. a repository authentication provider

   2b. an Oracle Access Manager Authentication provider

3. In this WebLogic Server configuration the username and password are sent to Active Directory for validation.
4. If Active Directory returns a successful validation to Oracle Management Service, via Oracle WebLogic Server, the user will gain access to the Enterprise Manager home page. If Active Directory returns an unsuccessful validation to Oracle Management Server, via Oracle WebLogic Server, the user will be denied access to Enterprise Manager.

This document focuses on the steps required to configure and validate users in to Enterprise Manager 12c using Active Directory.

Microsoft Active Directory

Active Directory is a directory store developed by Microsoft to operate in Windows domain networks. Active Directory controller provides centralized authentication and authorization for all users, throughout the entire network. Active Directory can also authenticate computers and enforce security policies. It determines which users are authorized to access different systems and applications through a single sign on.

One-step Configuration

Active Directory is one of three authentication schemes for which Enterprise Manager has provided one-step configuration. One-step configuration allows the necessary configuration parameters required for successful authentication to be set, in one command. One-step configuration sets the necessary parameters in Enterprise Manager and WebLogic Server. One-step configuration improves ease of use, enhances user experience, and reduces the chance of user configuration errors.

Enterprise Manager provides one-step configuration for the following popular authentication schemes:

1. Microsoft Active Directory
2. Oracle Access Manager
3. Oracle Internet Directory

One-step configuration is achieved using the `emctl` command. Running this command on the Oracle Management Service creates the specified authentication provider, e.g. “ad” creates an Active Directory authentication provider, “oid” creates an Oracle Internet Directory authentication provider, and “oam” creates an Oracle Internet Directory authentication provider.

One-step configuration for Active Directory creates an `ActiveDirectoryAuthenticator`. The `ActiveDirectoryAuthenticator` contains the necessary parameters required for successful user authentication and communication between Enterprise Manager and Active Directory. Any configuration values not specified retain the default values.

This document shall outline the steps involved in configuring Enterprise Manger and WebLogic Server to use Active Directory for external user authentication. Using Oracle Access Manager and Oracle Internet Directory for external authentication is beyond the scope of this document. Please refer to Enterprise Manager Security Guide for more information.

The `emctl` command requires the following information:

```
emctl config auth ad -ldap_host <ldap host> -ldap_port <ldap
port> -ldap_principal <ldap principal> [-ldap_credential <ldap
credential>] [-sysman_pwd <pwd>] -user_base_dn <user base DN> -
group_base_dn <group base DN>
```

Where:

`ldap_host`:	LDAP host name, this is the machine name where Active Directory has been installed. *Value used in our example: www.myadconsole.com*
`ldap_port`:	LDAP port, the active port where Active Directory is listening for requests *Value used in our example: 389*
`ldap_principal`:	The distinguished name (DN) of the Active Directory user the WebLogic server should use to connect to the LDAP server to ensure the users validity.
`ldap_credential`:	Password for the user specified by `ldap_principal` parameter
`sysman_pwd`:	This is the SYSMAN password and is required to set the necessary property value changes to Enterprise Manager
`user_base_dn`:	The base distinguished name (DN) of the tree in the LDAP directory that contains users. The users specified as the `ldap_principal` must have read access to this directory.
`group_base_dn`:	The base distinguished name (DN) of the tree in the LDAP directory that contains groups. The users specified as the `ldap_principal` must have read access to this directory.

Configuring Enterprise Manager

The following steps outline the steps, necessary for the successful configuration of Active Directory, WebLogic Server and Enterprise Manager:

1. Before running the following command, ensure the Active Directory LDAP server is up and running.
2. Run the `emctl config auth ad` command with the appropriate parameters. This command configures Enterprise Manager and WebLogic Server for successful external user authentication with Active Directory and was described in the previous section.

```
$>emctl config auth ad -ldap_host "myadconole.com" -ldap_port
"389" -ldap_principal
"cn=Administrator,cn=Users,dc=ys,dc=oracle,dc=com" -
ldap_credential "Welcome123" -user_base_dn
"cn=Users,dc=ys,dc=oracle,dc=com" -group_base_dn
"cn=Builtin,dc=ys,dc=oracle,dc=com" -sysman_pwd "sysman"

Oracle Enterprise Manager Cloud Control 12c Release 4
Copyright (c) 1996, 2014 Oracle Corporation.  All rights
reserved.
Configuring LDAP Authentication ... Started
Successfully validated connection to LDAP server
Configuring LDAP Authentication ... Successful
If this is a multi-OMS environment, restart all OMS(s)
using: 'emctl stop oms -all' and 'emctl start oms'
If use_ssl has been specified and the LDAP server
certificate is self-signed, as part of the validation
process, we have imported it into the keystore configured
for Weblogic Server.
```

3. We need to restart the Oracle Management Service to pick up the new configuration information. Stop the OMS.

```
$>emctl stop oms –all

Oracle Enterprise Manager Cloud Control 12c Release 4
Copyright (c) 1996, 2014 Oracle Corporation.  All rights
reserved.
Stopping WebTier...
WebTier Successfully Stopped
Stopping Oracle Management Server...
Oracle Management Server Successfully Stopped
AdminServer Successfully Stopped
Oracle Management Server is Down
```

4. Restart the OMS.

```
$>emctl start oms

Oracle Enterprise Manager Cloud Control 12c Release 4
Copyright (c) 1996, 2014 Oracle Corporation.  All rights
reserved.
Starting Oracle Management Server...
Starting WebTier...
WebTier Successfully Started
Oracle Management Server Successfully Started
Oracle Management Server is Up
```

Note: With Enterprise Manager configurations consisting of multiple Oracle Management Service instances, `emctl config auth ad` must be run on each OMS. Each OMS must also be restarted for changes to take effect.

WebLogic Server Tuning

As mentioned previously, one-step configuration allows for easier configuration of Enterprise Manager and WebLogic Server. This is done by using the “emctl config auth ad” command. In configuring Enterprise Manager for external user authentication using “emctl config auth ad” you are prompted to provide the machine names, port numbers, authorized administrators, their passwords and appropriate domain within AD where the users reside. For all other values, defaults are set.
The default values are selected as they are suitable for most environments. It is recommended that these default values be reviewed by the Active Directory administrator, to ensure they are suitable for your environment before going into production.

> ***Note:*** *Further tuning and modification of advanced AD configuration parameters is carried out through the WebLogic Server Administration Console and not the emctl config auth ad command. Further configuration may be required in situations where there are many user groups, where group nesting is required or where caching optimizations are necessary, such concerns may arise when many users are spread across many branches which need to be traversed. Such advanced configurations are beyond the scope of this document.*

Please refer to the Oracle Fusion Middleware – Performance and Tuning for Oracle WebLogic Server, for more information.

Testing the Configuration

With the steps outlined in Configuring Enterprise Manager section above, users should now be able to successfully log into Enterprise Manager using external authentication via WebLogic Server with Active Directory.

The following steps can be performed to ensure that `emctl` has correctly configured WebLogic Server and Oracle Enterprise Manager.

We will create a new user in Active Directory. Then login to WebLogic Server and Enterprise Manager to ensure that new user is visible. This will ensure correct end to end configuration.

1. **Login in to Active Directory Console.**

   Use the correct connection information provided by your Active Directory Administrator. This administrator must be a user with write access to Active Directory.
   In this example we are using the Remote Desktop connection tool. We enter the computer name where the AD resides, which is the same as the `-ldap_host` parameter used in the `emctl config auth ad` command. We also enter the name of the administrator authorized to access and administer the AD console.

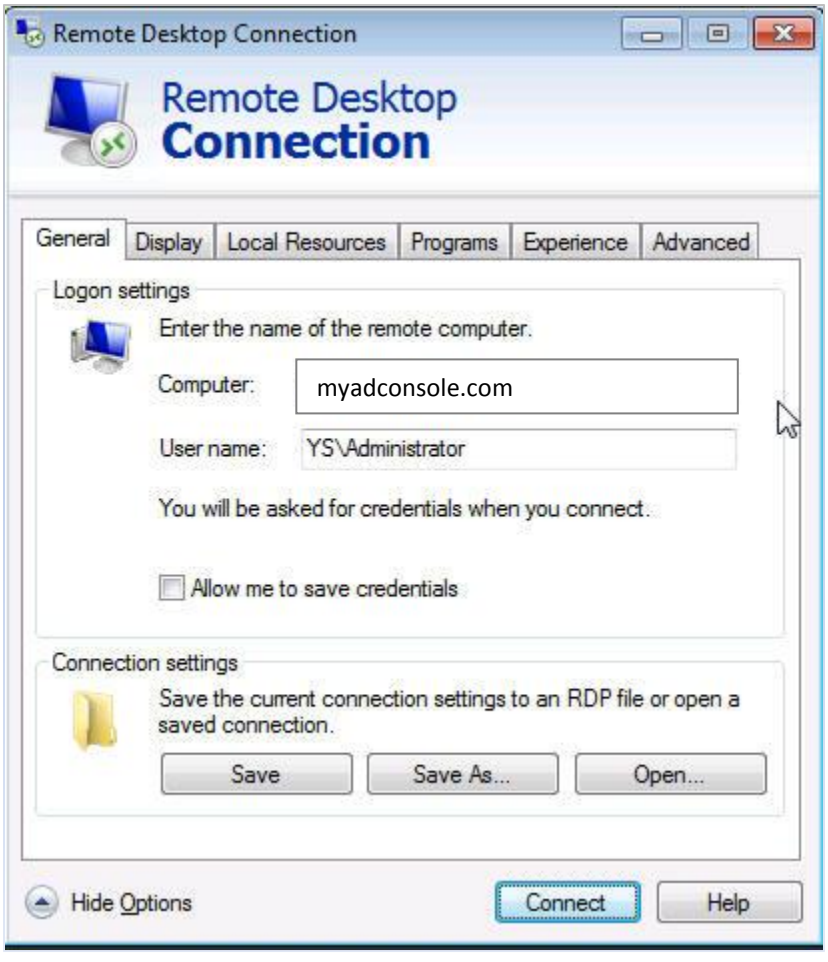

Figure 3: Using Remote Desktop to log into Active Directory

Once connected, navigate to the Users branch which contains the list of configured users. If configured correctly this list of users will also be displayed in the WebLogic Server console, and from which we will select those to grant access to Enterprise Manager.

2. **Creating a new User**
   For this example we have created a new user “Maureen Byrnem”. We did this by navigating to the users menu on the left hand side, right clicking on the user menu and following the directions for creating a new user. This can be seen in the image below. We shall grant “Maureen Byrnem” access to Enterprise Manager.

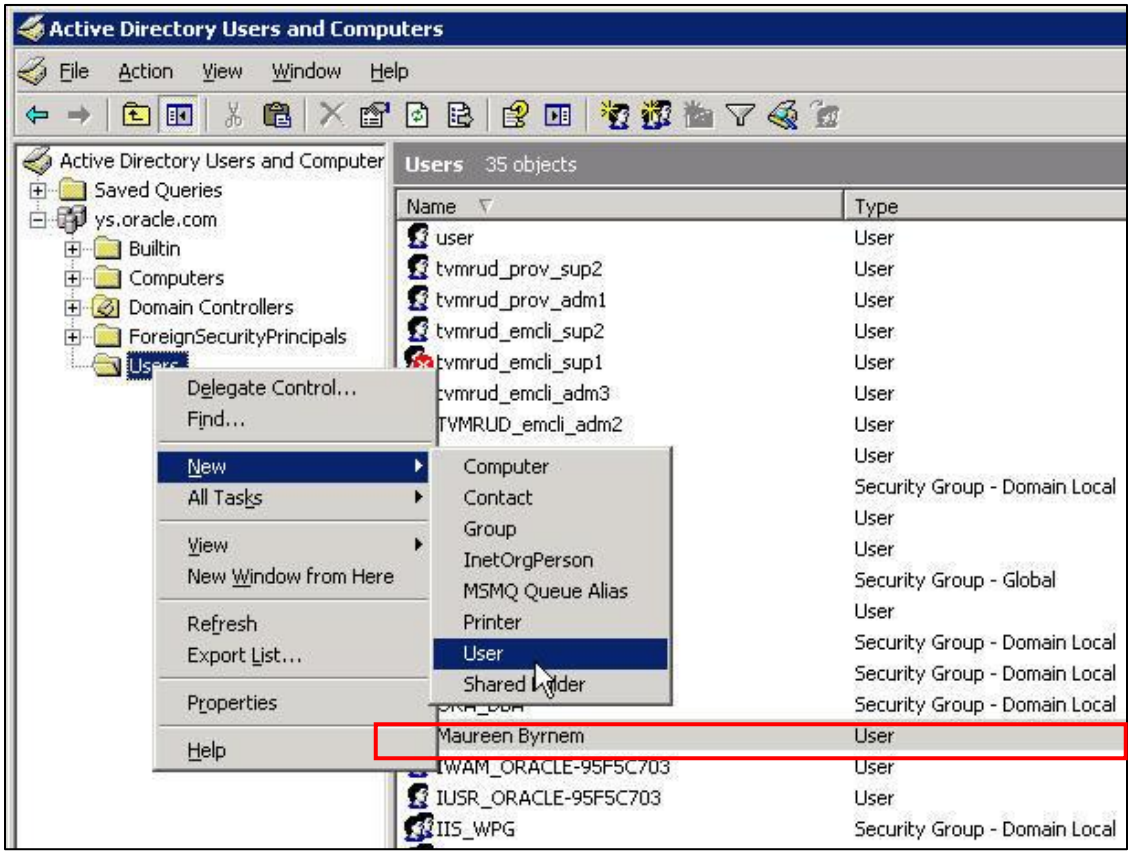

Figure 4: Creating a new user in Active Directory

3. **Log into WebLogic Server**

   Next we shall login to the WLS Console with the appropriate URL, as the administrator authorized to access the console.

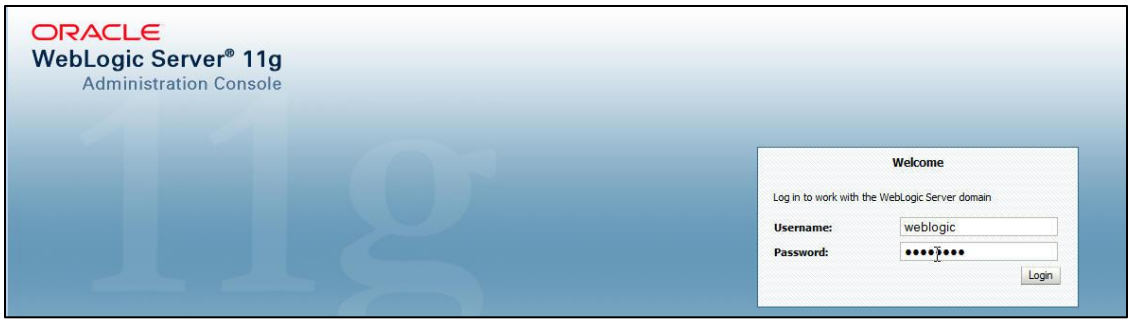

Figure 5: Logging into WebLogic Server Console

4. Observing the Security Realms

Navigate to the users group, from the Home page, select Services, Security Realms from the left hand side menu as shown in the image below.

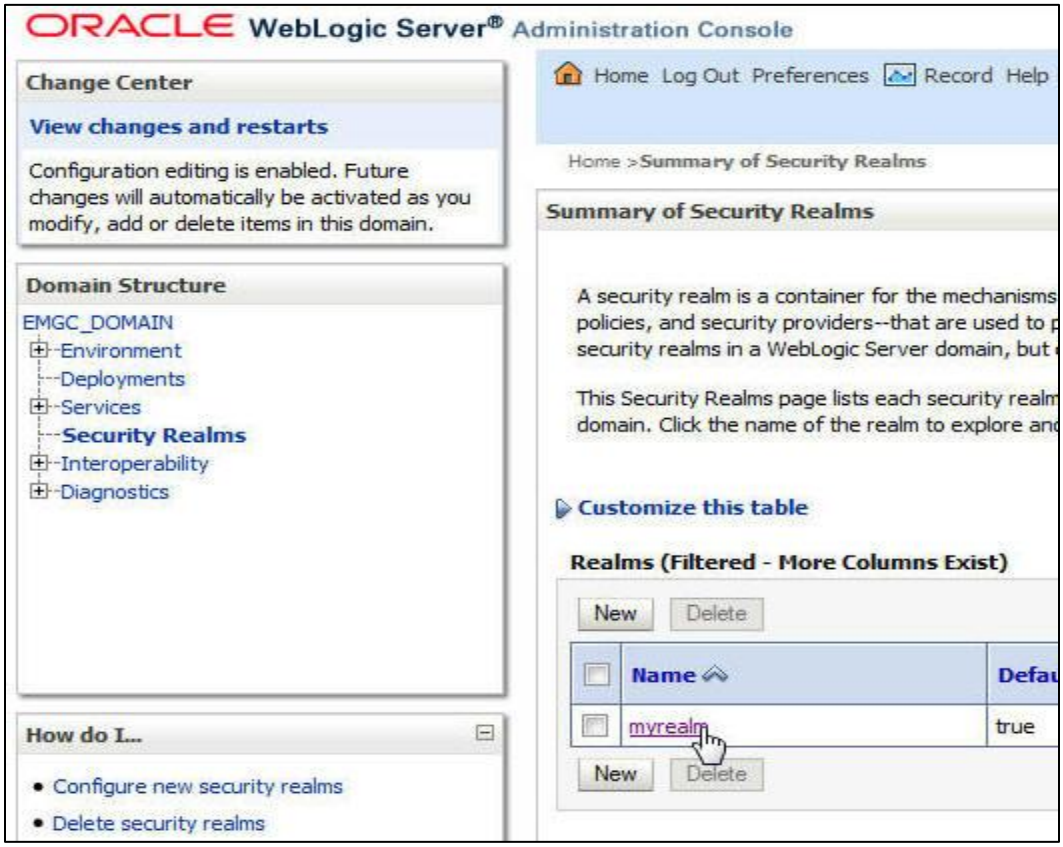

Figure 6: Observing the Security Reams in the WebLogic Server Console

Select the “myrealm” Realm from the table of listed Realms as shown in the image above, The Security Realms page lists each security realm that has been configured in this WebLogic Server domain.

5. Observing the User Groups

Select the “Users and Groups” tab from the top menu as shown in the image below. We see the newly created Active Directory user “Maureen Byrnem” displayed in the console.

Note: *for more detailed troubleshooting information on the WLS, navigate to the help, located at https://myfmws.com:17300/consolehelp/console-help.portal.*

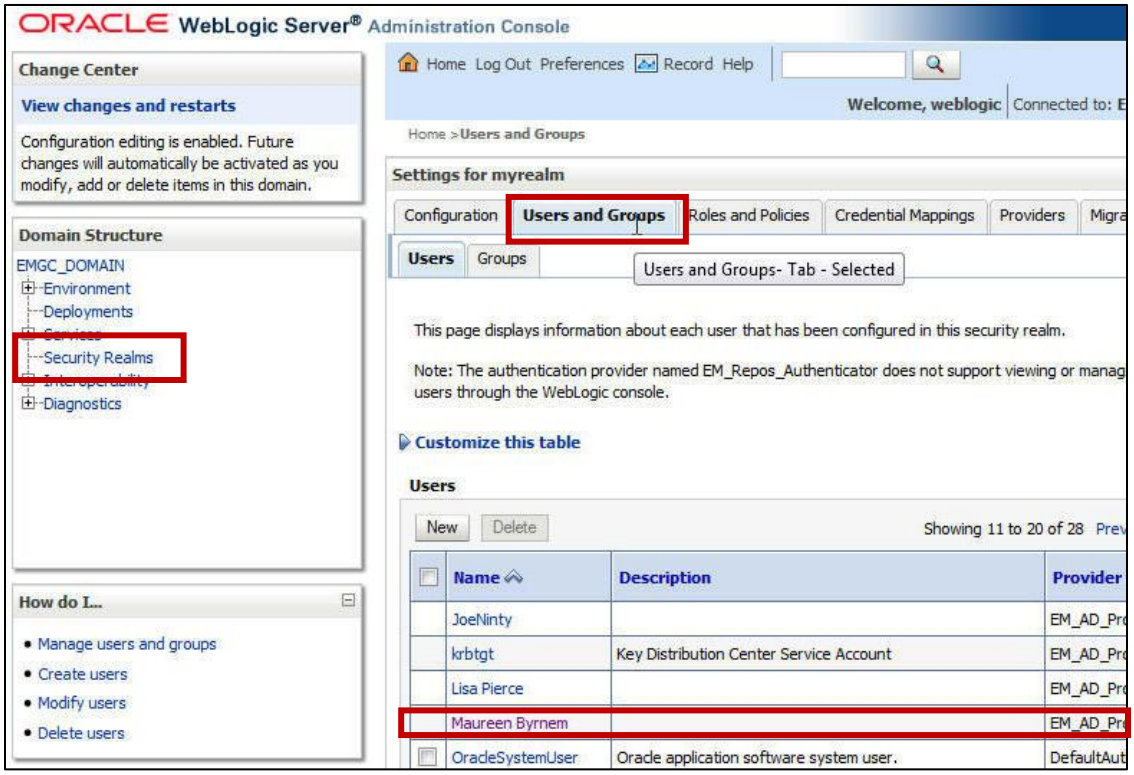

Figure 7: Observing the users in the WebLogic Server Console

4. Observing the Authentication Providers

Select the “Providers” tab from top menu – this lists the supported authentication providers for our Realm. Multiple providers can be configured for a Realm. You can click the name of the realm to explore and configure that realm. The Realms which are prefixed by “EM_” are those that have been configured and used by Enterprise

Manager. We can see our Enterprise Manager Active Directory Authenticator, EM_AD_Provider listed, after the EM_Repos_Authenticator.

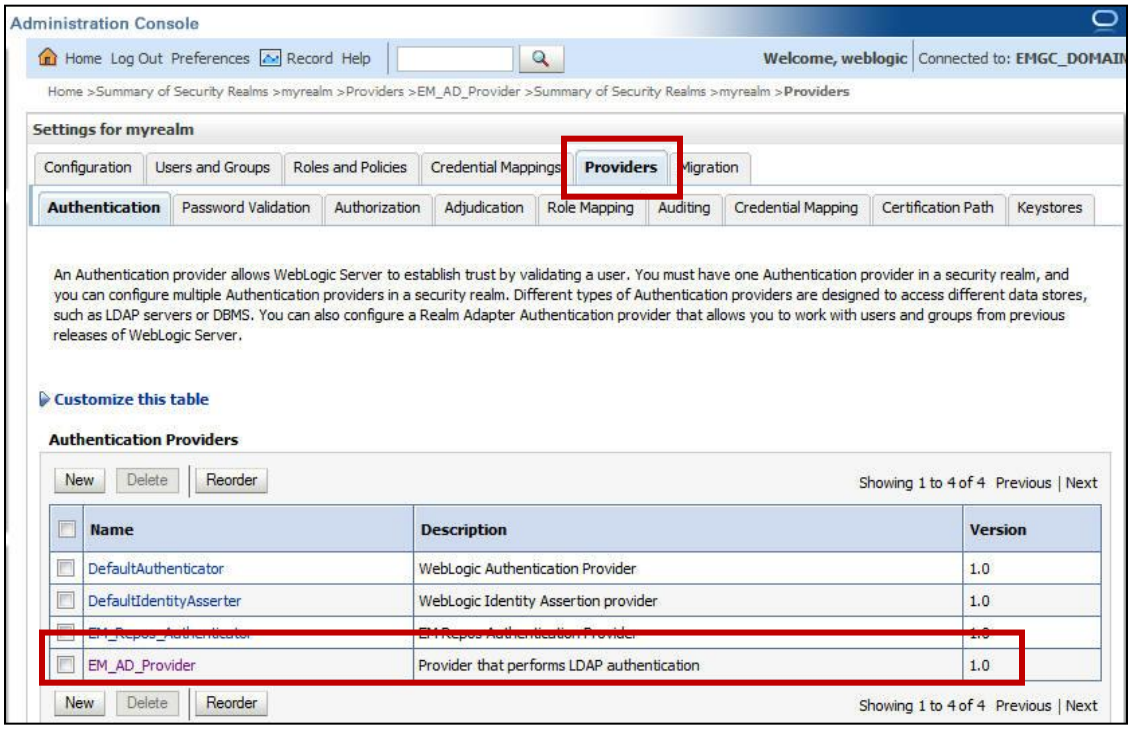

Figure 8: Observing the Enterprise Manager User Authentication Providers in WebLogic Server

The EM_Repos_Authenticator is provided out of box and is used to support Enterprise Manger repository authentication. The EM_AD_Provider was created when we ran the `emctl config auth ad` command. This is also an indicator that the `emcli config auth ad` command was successful.

During the authentication process WebLogic Server will try to authenticate a user, based on the order of these providers, and on the value of the “Control Flag”. The “Control Flag” property determines the priority and user authentication criteria defined in the Authentication provider. WebLogic Server will use these values to determine if one or many providers are needed to successfully authenticate a user.

5. Reviewing the EM_AD_Provider

Click on the `EM_AD_Provider` Authentication Provider. Here we see more specific information about the `EM_AD_Provider`. We see the Control Flag has a value of “SUFFICIENT”, indicating that Enterprise Manager will iterate through the authentication providers listed until it can authenticate the user. If the

`EM_AD_Provider` is successful in authenticating the user no other providers will be tried, if it fails it will simply more on to the next provider listed in WebLogic Server.

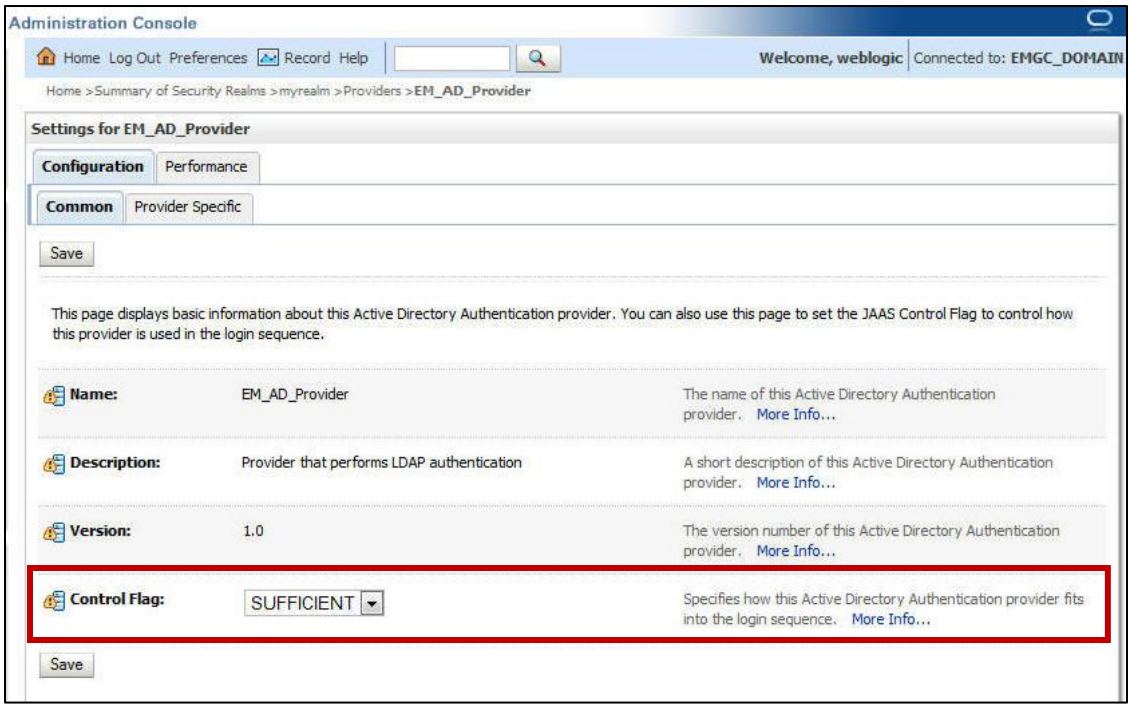

Figure 9: Observing the EM_AD_Provider *Providers in the WebLogic Server Console*

Next proceed to the “Provider Specific” tab at the top menu. Here you will see all the information that was specified during the `emctl config auth ad` command, such as the LDAP host name, port number and the AD principal.
This is yet another indicator that `emctl config auth ad` was successful.

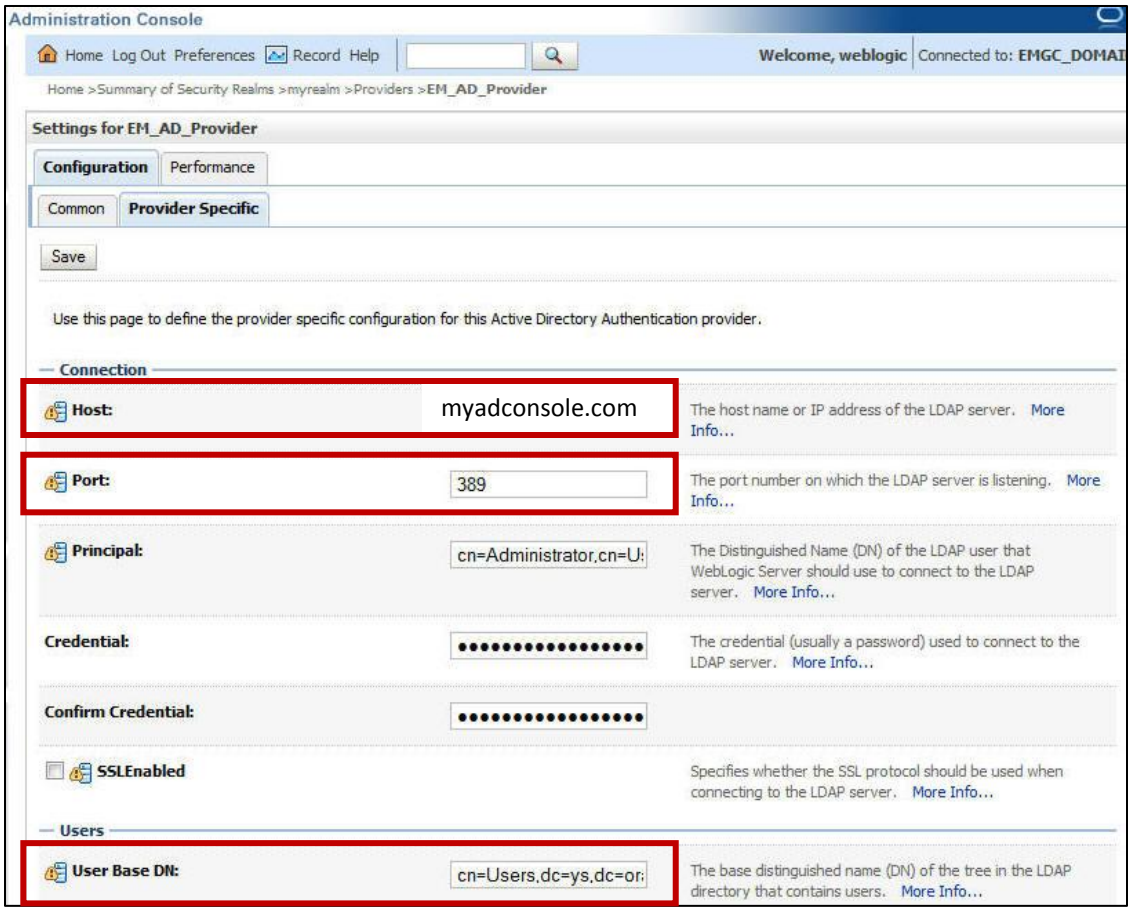

Figure 10: Observing the EM_AD_Provider *Providers configuration parameters in the WebLogic Server Console*

6. Validating Enterprise Manager Configuration

Next we ensure that Enterprise Manager has been configured to allow external authentication. We do this by ensuring the necessary Enterprise Manager Oracle Management Service properties have been set, these are

```
oracle.sysman.core.security.auth.is_external_authentication_ena
bled = true
```

and

```
oracle.sysman.emSDK.sec.DirectoryAuthenticationType = LDAP
```

These parameters will have been set by `emctl config auth ad` command.

Login to Enterprise Manager as the Super Administrator. Navigate to the management Services by selecting Setup->Mange Cloud Control->Manage Services, as indicated in the image below.

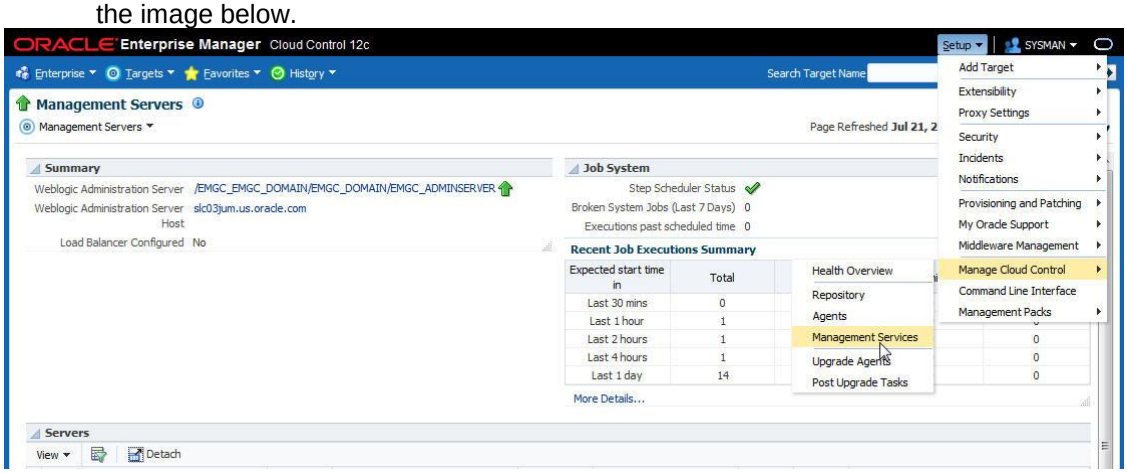

Figure 11: Navigating to the Management Services page in Enterprise Manager

Once you have arrived at that page, navigate to the configuration properties page by selecting Management Servers->Configuration properties, as indicated on the image below.

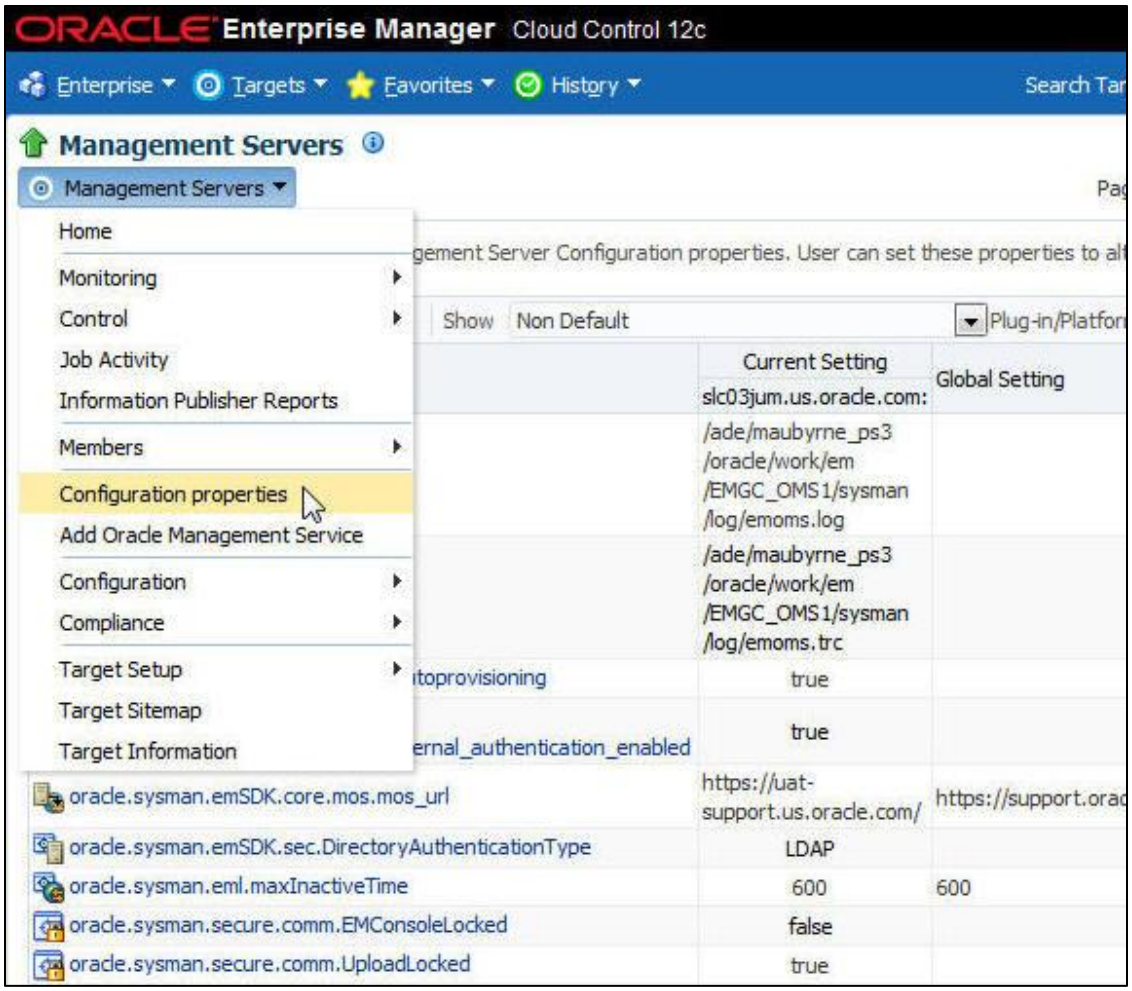

Figure 12: Observing the Configuration Parameters page in Enterprise Manager

Once on this page we can verify that the parameters are set correctly.

oracle.sysman.core.security.auth.is_external_authentication_enabled= true

and

oracle.sysman.emSDK.sec.DirectoryAuthenticationType=LDAP

as indicated in the image below.

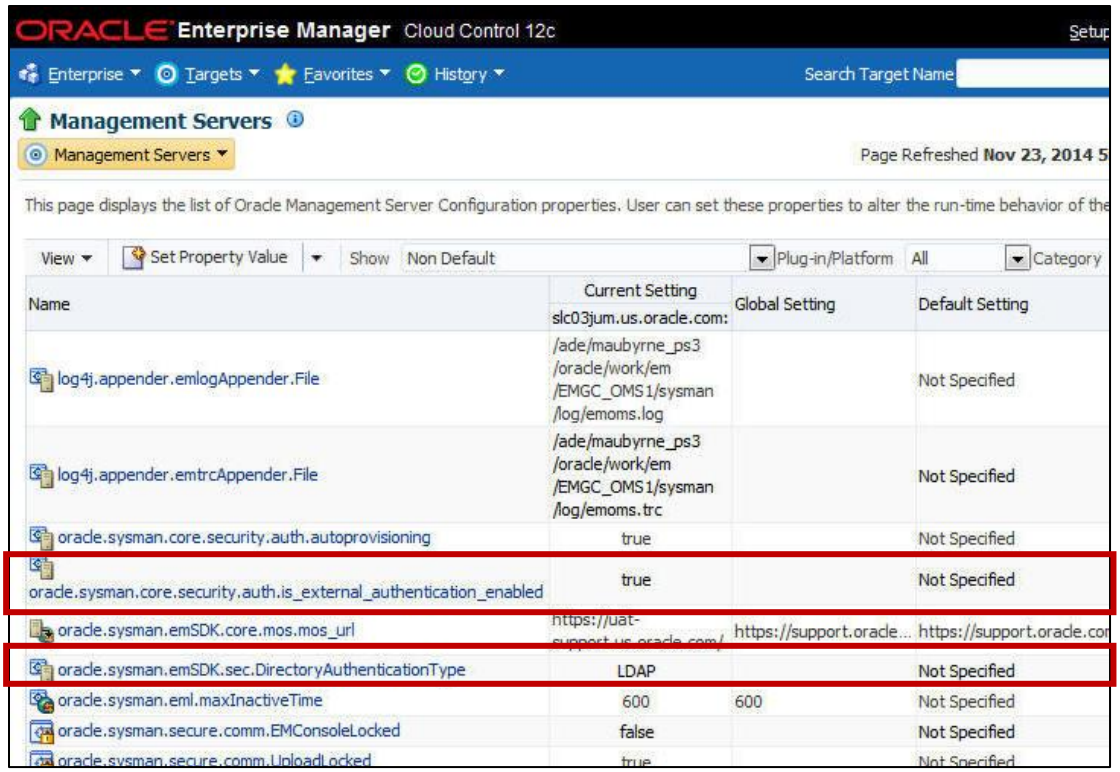

Figure 13: Observing the Configuration Parameters page in Enterprise Manager

7. Creating a User Account to Enterprise Manager

Next we must ensure that the newly created (external) user is authorized to access Enterprise Manager. The Super Administrator does this by creating a new (external) user by selecting Setup->Security->Administrator, from the right hand top menu, as indicated in the below image. Once on this page, select the “create” button.

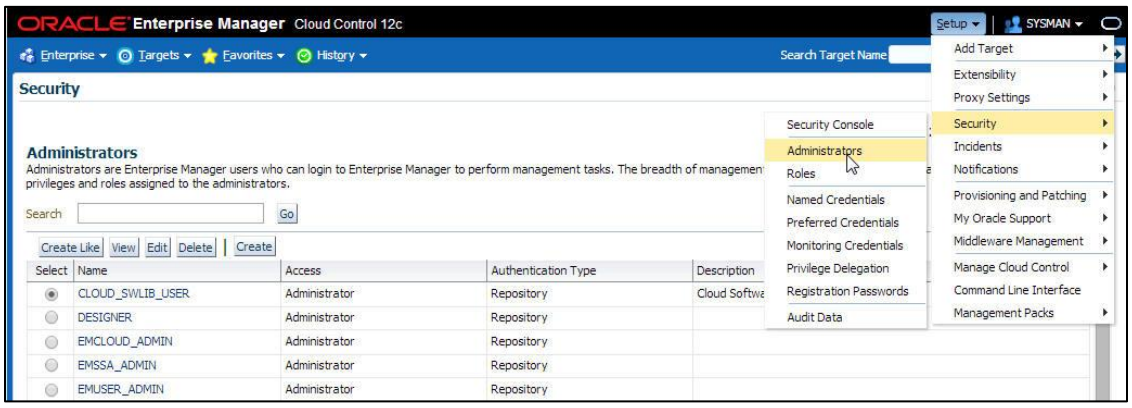

Figure 14: Navigating to the new administrator page in Enterprise Manager

This brings the Super Administrator to the “Create Administrators: Properties” page.

When external authentication is enabled a magnifying glass will display on the page next to the name window. Select this icon.
Enter the user name. I have entered “Maureen Byrnem”. This is as it was in the Active Directory and WebLogic Server Consoles, as indicated in the image below.

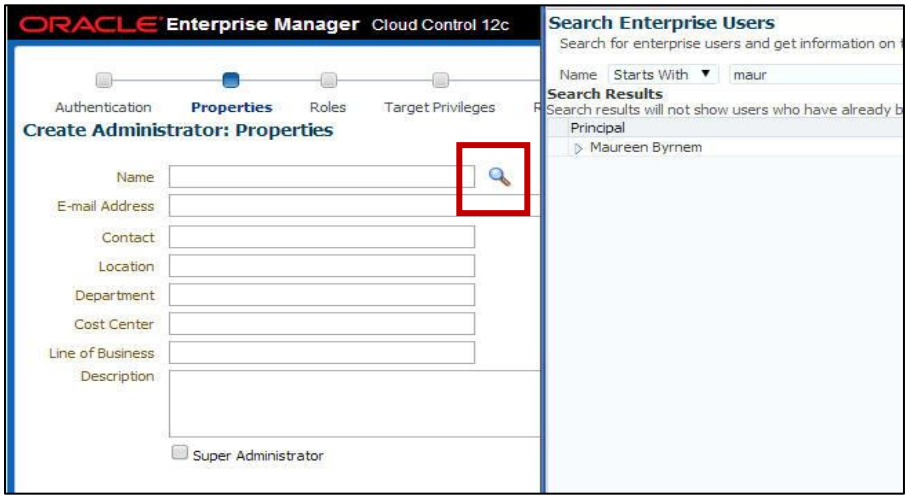

Figure 15: Creating an External User in Enterprise Manager

Next we select the “Review” button and select “OK”. The new (external) user is now authorized to access the system.

8. Validating User Access to Enterprise Manager

Next we shall verify that “Maureen Byrnem” can successfully access Enterprise Manager. Log in as the newly created user, and entering the password specified during user creation in Active Directory.

Figure 16: Logging into Enterprise Manager as a newly created External User

Upon successful login the new (external) user arrives at the Enterprise Manager home page. Seeing the user name “Maureen Byrnem” on the top right hand corner indicates successful login and configuration.

This ensures that Enterprise Manager Cloud Control 12c has been correctly configured to use Active Directory for User Authentication.

Please refer to the Enterprise manager Security Guide for more information.

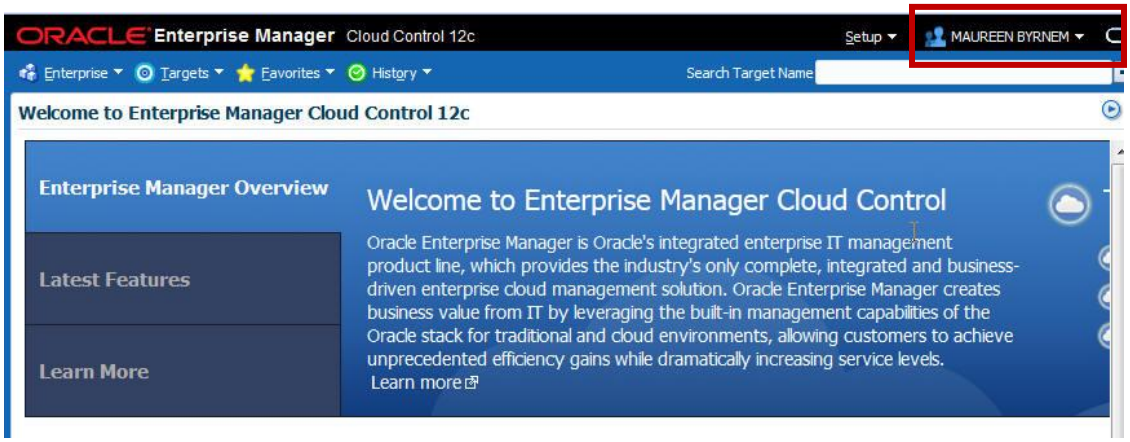

Figure 17: Observing the Username in Enterprise Manager

***Note:** Management of an externally authenticated AD users’ password is changed at any time by right clicking the username in the AD console and selecting “reset password” and following the directions.*

Auto-provisioning

Auto provisioning in Enterprise Manager is a feature where externally authenticated LDAP users do not have to be provisioned (pre-created) manually in Enterprise Manager. The user account is auto created when the users first log in is successful.
Auto provisioning, if enabled, applies to all successful externally authenticated users upon first login. Auto provisioning is enabled by setting the Oracle Management Service, OMS, property “`oracle.sysman.core.security.auth.autoprovisioning`” to true, as follows.

```
$>emctl set property – name
oracle.sysman.core.security.auth.autoprovisioning –value true
```

This property can also be set using Enterprise Manager Command Line Interface, EM CLI, as follows

```
emcli>set_oms_property -property_name=
oracle.sysman.core.security.auth.autoprovisioning -
property_value=true
```

This property can also be set in the console by navigating to the Management Services page and selecting the `oracle.sysman.core.security.auth.autoprovisioning` property and setting it to true, as indicated in the images below.

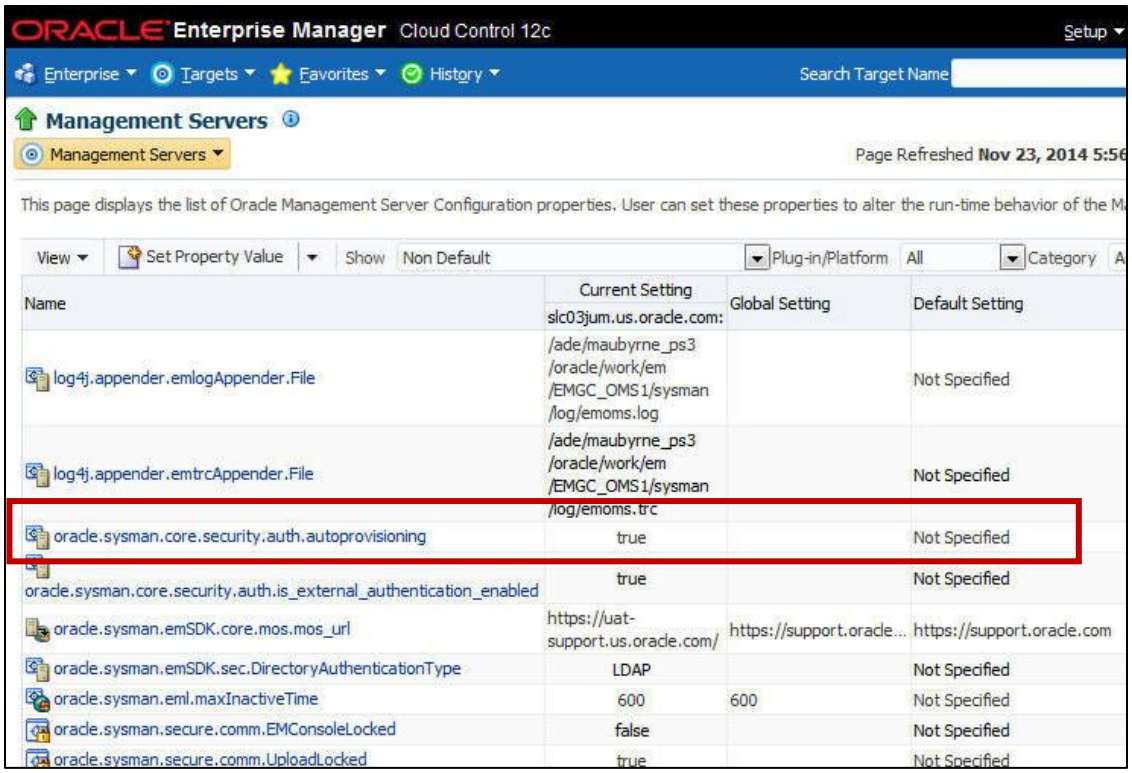

Figure 18: Observing Oracle Management Service properties in Enterprise Manager

Once you have selected the property it will bring you to a page which will allow you to edit the property.

Auto provisioning can be configured to apply to all new users or it can be configured to apply to a reduced set of users, i.e. auto-provisioning of users which are present in a specific Active Directory group only, by setting the Oracle Management Service property "`oracle.sysman.core.security.auth.autoprovisioning_minimum_role`" as follows.

```
oracle.sysman.core.security.auth.autoprovisioning_minimum_role =
<LDAP group Name>
```

for example:

```
$>emcli set property -name
oracle.core.security.auth.autoprovisioning_minimum_role -value
EM_ADMIN_USERS
```

The LDAP group name refers to a group of users in LDAP/Active Directory who will be auto provisioned upon their first successful login in. This means that only users listed in this will be

auto provisioned when they log in, all other user accounts will need to be pre-created, prior to their login. This might be useful in an organization which had a dedicated group of Oracle DBAs or EM Administrators who rely on access to Enterprise Manager to perform their daily tasks. These OMS properties can be set via the console UI or EM CLI as indicated in step 6 of the Testing the Configuration section above.

External Roles

When configured for external authentication Enterprise Manager can also be configured to allow Active Directory to manage authorization. Authorization determines what actions a user can perform in Enterprise Manager and on managed targets. Authorization in Enterprise Manager is defined using role based access control and fine grained privileges.
External roles in Enterprise Manager allow a group of users defined in LDAP/Active Directory, to be assigned a role when a user from the Active Directory group logs into Enterprise Manager.
External Roles enhance ease of use and integration, especially in organizations where authorization is already being managed by the Active Directory administrator.

A role is created in Enterprise Manager from the Setup->Security->Roles menu page. Checking the "external role" box – indicates the role is an external role. The name of the external role in Enterprise Manager is the same as an existing user group name in Active Directory, in which the authenticating user resides. The role in Enterprise Manager defines the necessary privileges which will be auto-assigned to that user upon successful log in to Enterprise Manager. This allows the user to change groups in Active Directory and for his role (and privileges) to seamlessly change (upon his next successful login) and propagated in Enterprise Manager. When used with auto-provisioning it allows a user to be auto-assigned the necessary privileges for him to perform his job in Enterprise Manager.

The following series of steps guide us through creating an external role in Enterprise Manager.

1. **Creating a Group of User**

   Let's login to Active Directory to create our group of users. These users will be granted the external role when they log in to Enterprise Manager. Once logged into Active Directory. Navigate to the group directory that was defined in the "`emctl config auth ad ...`" command at the beginning of this document. To recap, the command was (from step 2 of the Testing your Configuration section, creating a New User, above) as follows

   ```
   $>emctl config auth ad -ldap_host "myadconole.com" -ldap_port
   "389" -ldap_principal
   "cn=Administrator,cn=Users,dc=ys,dc=oracle,dc=com" -
   ldap_credential "Welcome123" -user_base_dn
   "cn=Users,dc=ys,dc=oracle,dc=com" -group_base_dn
   "cn=Builtin,dc=ys,dc=oracle,dc=com" -sysman_pwd "sysman"
   ```

   Our directory structure is indicated in the image below on the left hand Navigation menu, the name of our user directory is "Builtin".

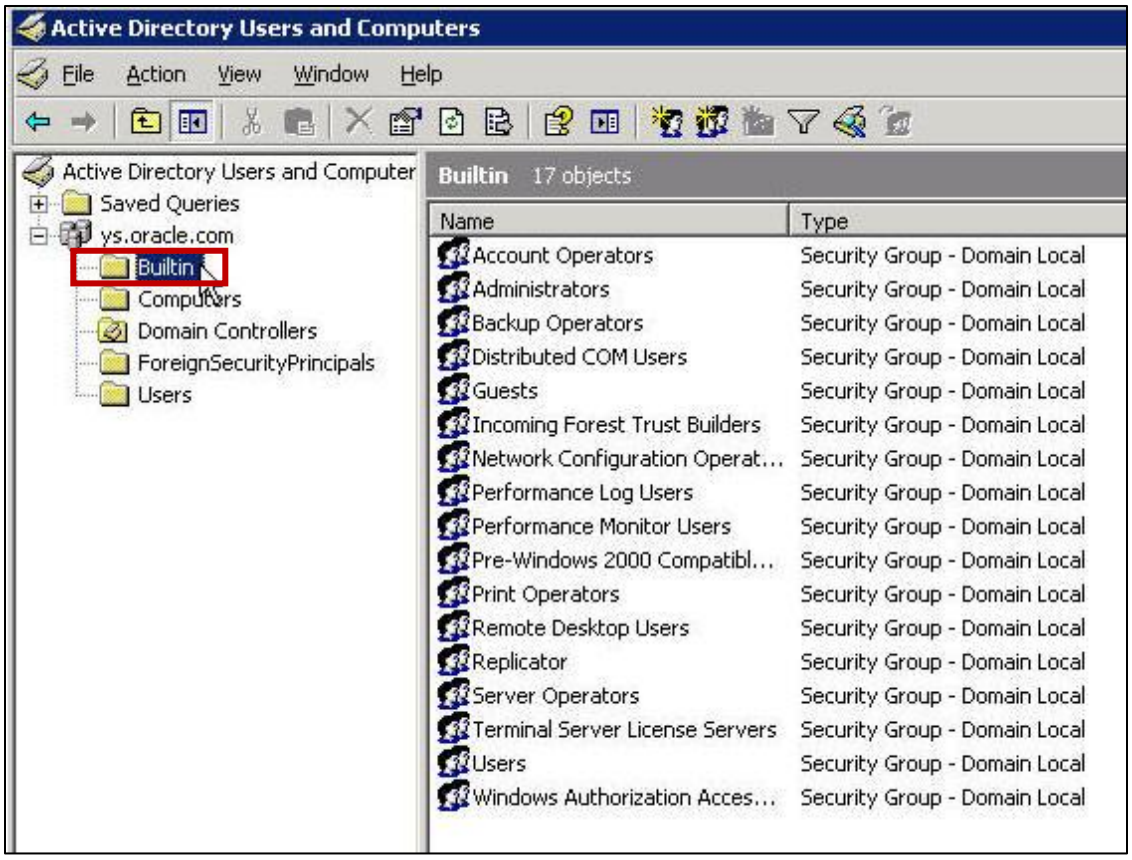

Figure 19: Navigating to user groups in Active Directory

Let us create a new user group with the name EM_ADMIN, this group name will match the name of the external role we will define in Enterprise Manager. You can create a new group by right mouse clicking in the directory and navigating to the New->Group menu item, as indicated in the image below.

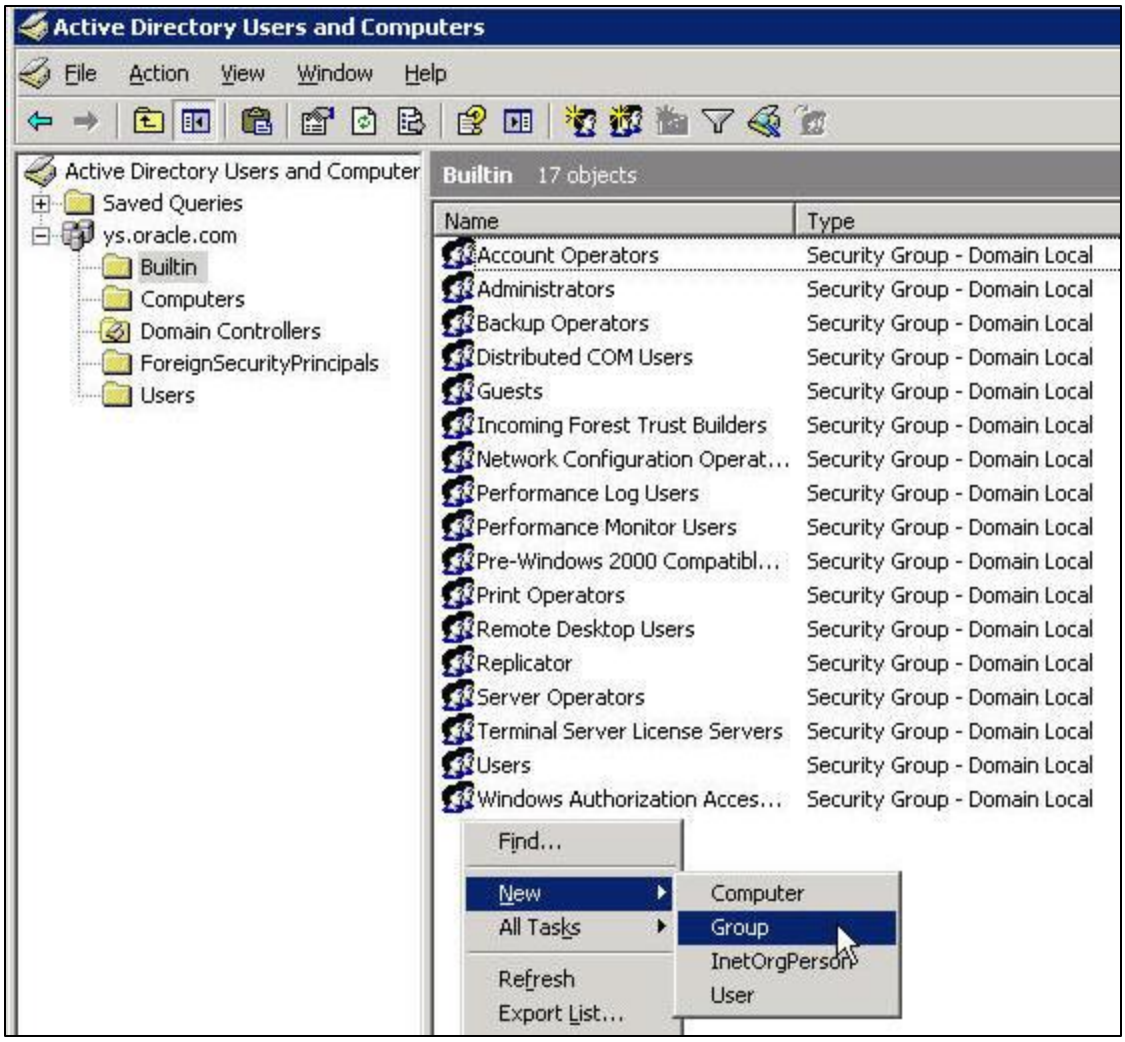

Figure 20: Creating a new user group in Active Directory

Add users to this group. I have created a new user called “Tom Jones” and added him to the EM_ADMIN group. I have also added our “Maureen Byrnem” user to the group.

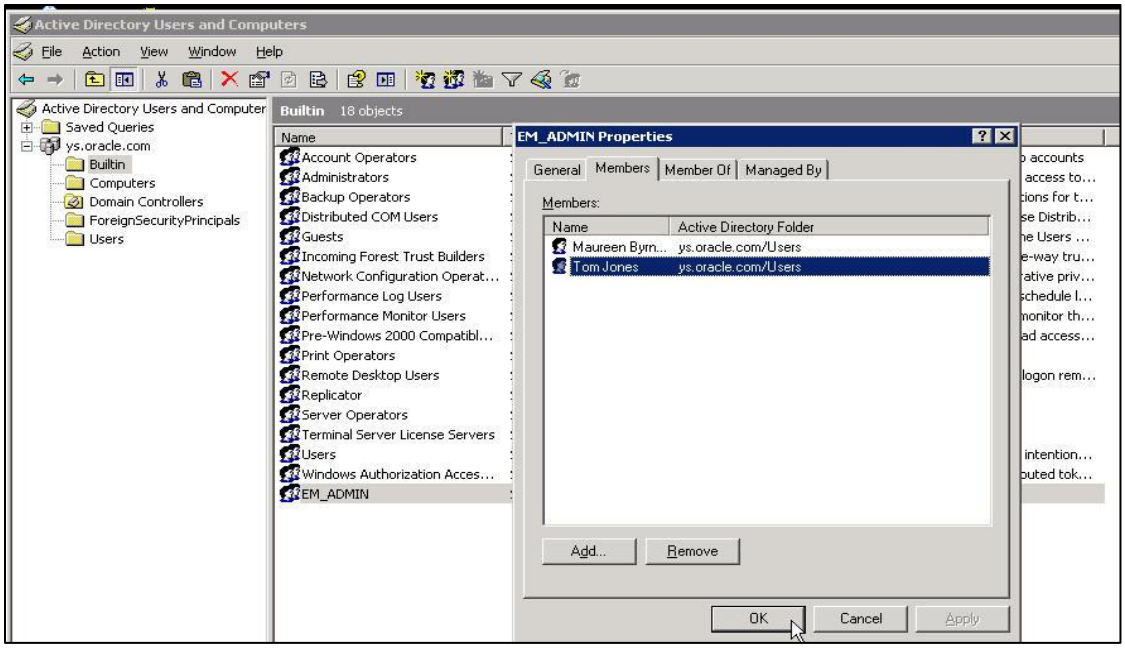

Figure 21: Adding users to a user group in Active Directory

2. Creating an external role

Let's create our EM_ADMIN role and define the privileges for that role. Navigate to the roles page in Enterprise Manager as indicated in the image below, by selecting Setup->Security->Roles.

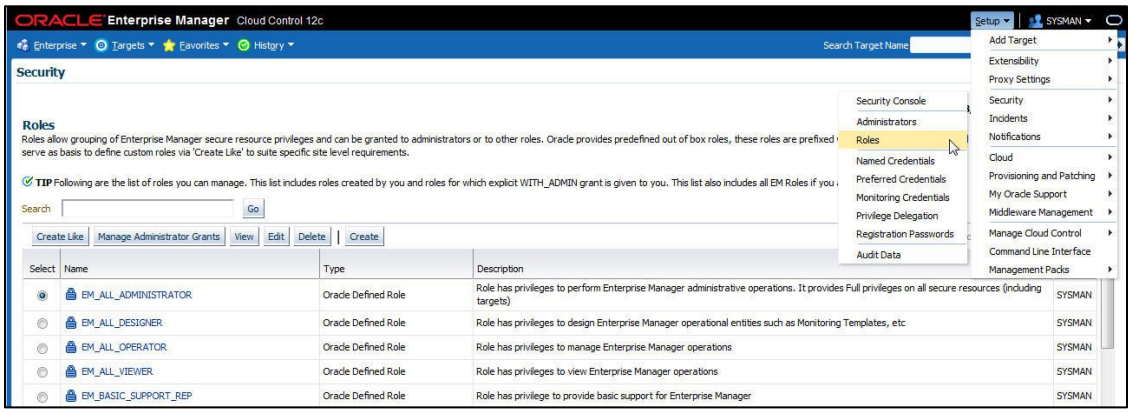

Figure 22: Navigating to the roles page in Enterprise Manager

Create a role and mark it as "external" by selecting the external role box, as indicated in the image below. This external role name must match the LDAP group name where the users are defined. When these users login to Enterprise Manager they will be granted the specific privileges as defined by the EM_ADMIN role.

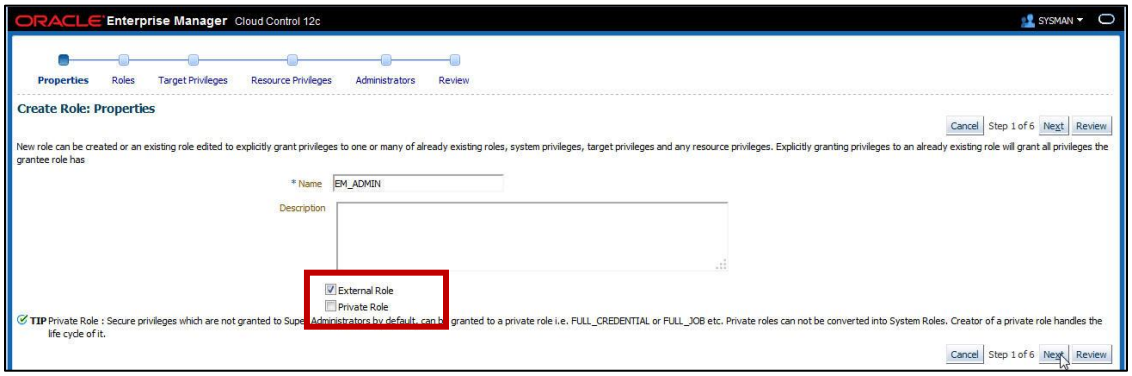

Figure 23: Marking a role as external on roles page in Enterprise Manager

I created the EM_ADMIN role and defined the VIEW privilege on one database only. The review page indicates that EM_ADMIN is an external role. Select Save.

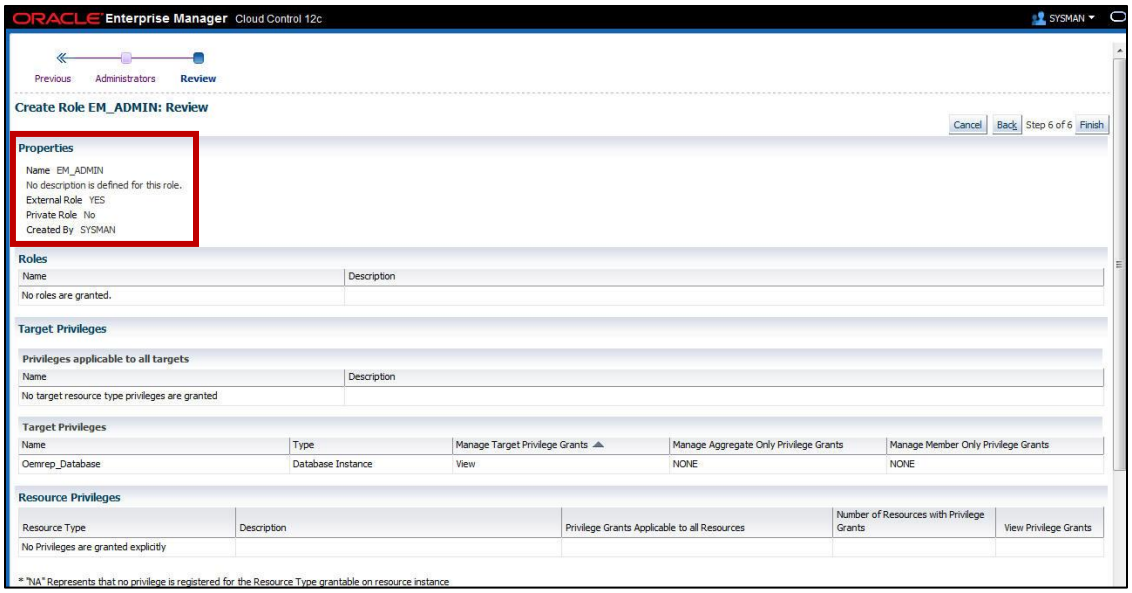

Figure 24: Observing the Entitlement page in Enterprise Manager

3. Validating external role and auto-provisioning

As I also have auto-provisioning turned on when “Tom Jones” logs into Enterprise Manager his account information will be created and provisioned for him, he will also be granted the privileges defined in the external role EM_ADMIN upon first successful login.

Figure 25: Logging in as a new user in Enterprise Manager

Note that “Tom Jones” username is the same as that specified in the “Display name” field of the “General” section, and that displayed in the “Users” list when creating a new user in Active Directory, as indicated in the image of the Active Directory console below.

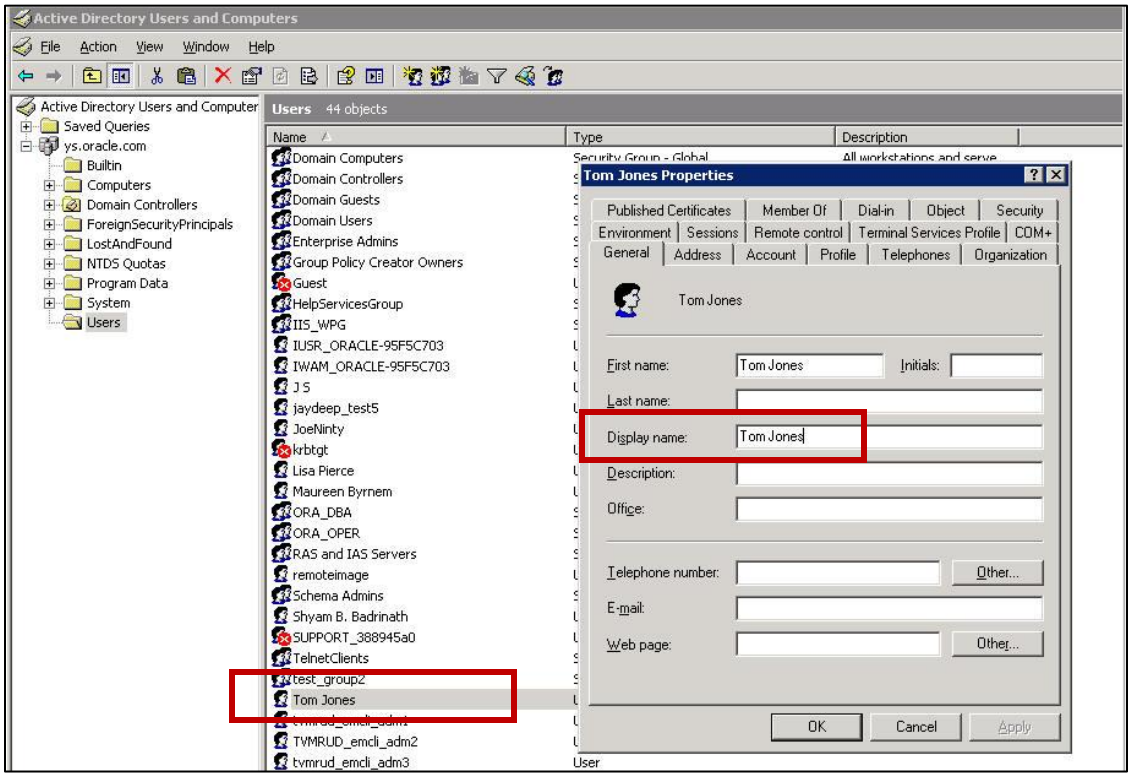

Figure 26: Observing the new user name in Active Directory

Log into Enterprise Manager as Tom Jones. Navigate to the Entitlement Page at the the top tight hand corner, under the “name” menu, as indicated in the image.

Figure 27: Observing the new user name and Navigating to the Entitlement Page in Enterprise Manager

On the Entitlement page you will see the external role name listed in the “Granted Roles” table as indicated in the image below.

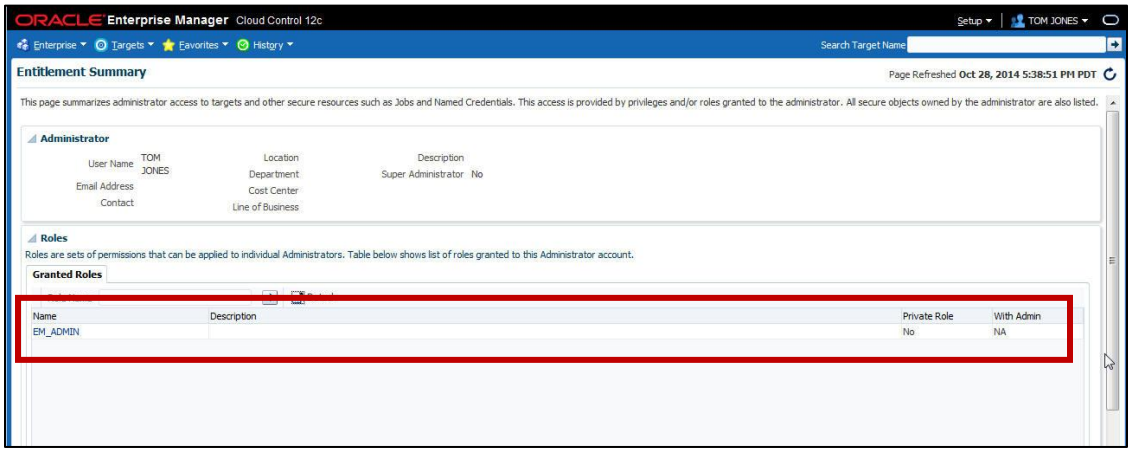

Figure 28: Observing the external role name on the Entitlement Page in Enterprise Manager

This indicates that “Tom Jones” had been granted the EM_ADMIN external role. “Tom Jones” successful login without his user account being pre-provisioned indicates he is an externally authenticated, auto-provisioned user, who is also a member of the EM_ADMIN user group in Active Directory.

Active Directory Advanced Configuration

Active Directory and Enterprise Manger have other key integration enhancements which improve usability, but are beyond the scope of this document.
They include:

1. Mapping NumericIDs to UserNames
2. Mapping LDAP user attributes to Enterprise Manager attributes
3. How To Configure the WCC Domain Active Directory Provider to Use sAMAccountName (MOS Doc ID 1519267.1)

Please see the Enterprise Manager Security Guide for further information on the first two features, and My Oracle Support for the last item listed.

Version Information

The screenshots captured in this white paper were performed while using the following application versions.

Software	**Version**
Microsoft Active Directory	5.23790
Microsoft Management Console	3.0
Oracle WebLogic Server Console	10.3.6.0
Oracle Enterprise Manger Cloud Control	12.1.0.4

Figure 29: Version information of software used

Referenced Links

Oracle Enterprise Manager Cloud Control Administrator’s Guide
Oracle Fusion Middleware Administrator’s Guide
Oracle Fusion Middleware Securing Oracle WebLogic Server
Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server
Microsoft Active Directory Documentation
Oracle Enterprise Manager Cloud Control Security Guide
Oracle Fusion Middleware – Performance and Tuning for Oracle WebLogic Server

Oracle Enterprise Manager Cloud Control 12*c*
Infrastructure and Operational Security Best Practices
June, 2015Author: Oracle
Contributing Authors: Courtney Llamas, Werner De Gruyter, Andrew Bulloch, Ravi Pinnamaneni

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together